

Remarks

Reconsideration of this application is requested in view of the foregoing amendments, the following remarks and the attached request for continued examination.

The status of the claims after the above amendments is as follows:

Claims 45-54, and 56 85 are pending and have been finally rejected; and
Claim 55 has been cancelled.

The examiner is thanked for the courtesy extended to the undersigned during a telephone interview conducted on December 17, 2009. During that interview the pending claims were discussed as well as the final rejections. While no agreements were reached during the interview, the examiner did indicate that he viewed the claim as a "black box" and that more specificity of the steps relating to the modeling and also the simulation phases would help to distinguish the claims from the cited art. The examiner will notice that claim 55 has been incorporated into claim 45 and also that we have now indicated that the method creates a virtual system on which to run the simulation and that the simulation phase specifies a series of potential attacks based on attack path elements. Further the state of a component of the information system altered by a successful attack is updated. Support for these amendments are in claim 55, page 17, lines 10-17, page 2, lines 30-32, and page 18, lines 15-26. No new matter has been introduced by the above amendments to either claims 45 or 83.

The examiner has rejected claims 45-48, 52, 53, 55, and 83 under 35 U.S.C. §103(a) as unpatentable over "Network Security Modeling and Cyber Attack Simulation Methodology" to Sung et al. published 7/11/2001, hereafter "Sung" in view of "Checkmate Network Security Modeling" to Apostol et al. published 6/12/2001, hereafter "Apostol". This rejection as it applies to the amended claims is traversed.

As recognized by the examiner in the office action, Sung does not show that each initialized state corresponds to the security status and that a successful attack causes a state to change. The examiner considers that Apostol shows these missing elements. In the context of claims 45 and 83, Sung does not show creation of a virtual system to be used in the simulation and also does not show construction of a local routing table. Apostol only has very general disclosure of the hoped for

outcome of an attack, that the state of a device can be changed to allow an attacker to exploit a vulnerability. Apostal does not show “updating the state of a component of the information system altered by a successful attack, wherein a successful attack causes a state of a component to pass to an unsound value” as required by claims 45 and 83. Further, Apostal only discloses the state of service on specific nodes but this does not disclose the status of the node regarding security in the context of attacks launched against the system. There is no disclosure of the claimed states corresponding to security status of each component in the context of attacks launched against the system. The states as used in the present system reflect a value assigned to the component to reflect that component’s security status relative to a proposed attack. This is different from the status itself. As such Apostal does not make up the admitted deficiencies of Sung noted by the examiner in the office action and the rejection of claims 45-48, 52, 53, 55, and 83 is unwarranted and should be withdrawn.

The examiner has also rejected claims 49-51 and 54 under 35 U.S.C. §103(a) based on the combination of Sung and Apostal discussed above and further in view of Richey et al. “Using model checking to analyze vulnerabilities,” hereafter Rickey. This rejection is traversed.

Rickey does not remove the deficiencies of Sung and Apostal relative to claim 45 and because these claims are dependant on claim 45, these claims also should be allowable.

The examiner has also rejected claims 56, 57, 59-61, 67-69, 71-73, 84 and 85 under 35 U.S.C. §103(a) based on the combination of Sung and Apostal discussed above and further in view of Gupta et al, US7289456, hereafter “Gupta”. This rejection is traversed.

It should be noted that Gupta does not remove the deficiencies of the Sung Apostal rejection of claims 45 and 83. Gupta does not relate to defending attacks on a system and is interested in modeling a system to improve network efficiency. The fact that a system can determine the shortest path in a network does not disclose or suggest that this issue is important from a security view in terms of defending a system from cyber attack. Because Gupta does not remove the deficiency of the rejection of claims 45 and 83, from which all the rejected claims depend, this rejection is no longer warranted.

Claims 58, 70, 74-76, and 77-82 are rejected under 35 U.S.C. §103(a) based on the Sung Apostal combination combined with Gupta and one or more of US7315801, US6952779,

US6061505, and US7013395. As noted above Sung and Apostol do not render claim 45 obvious because of a failure of disclosure. None of the added patents makes up for this inadequate disclosure and therefore, the rejection of these claims is unwarranted and should be withdrawn.


If there are any issues remaining that can be resolved by telephone, the examiner is invited to call the undersigned.

Deposit Account Authorization

The Commissioner is hereby authorized to charge any deficiency in any amount enclosed or any additional fees, which may be required during the pendency of this application under 37 CFR 1.16 or 1.17, except issue fees, to Deposit Account No. 50-1903.

Respectfully submitted,

MCCRACKEN & FRANK LLP
311 South Wacker Drive
Suite 2500
Chicago, IL 60606
(312) 263-4700
Customer No: 29471

By: 

J. William Frank, III
Reg. No. 25,626

January 21, 2010